PATENT

UNITED STATES PATENT APPLICATION

FOR

METHOD AND APPARATUS FOR IMPLEMENTING REVOCATION IN BROADCAST NETWORKS

Inventors:

Brant L. Candelore
Mark Eyer

prepared by:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 Wilshire Blvd., 7th Floor
Los Angeles, California 90025-1026
(408) 720-8598

Attorney Docket No.: 080398.P253

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number EL 234 215 981 US

Date of Deposit February 15, 2000

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231

Tina Domingo
(Typed or printed name of person mailing paper or fee)

2-15-2000
(Signature of person mailing paper or fee) Date

METHOD AND APPARATUS FOR IMPLEMENTING REVOCATION IN BROADCAST NETWORKS

BACKGROUND OF THE INVENTION

1. *Field of the Invention*

The present invention relates to digital devices. More specifically, the present invention relates to a copy management system and method for controlling the reproduction and recording of digital content on and from at least one digital device.

2. *General Background*

Analog communication systems are rapidly giving way to their digital counterparts. Digital television is currently scheduled to be available nationally to all consumers by the year 2002 and completely in place by the year 2006. High-definition television (HDTV) broadcasts have already begun in most major cities on a limited basis. Similarly, the explosive growth of the Internet and the World Wide Web have resulted in a correlative growth in the increase of downloadable audio-visual files, such as MP3-formatted audio files, as well as other content.

Simultaneously with, and in part due to, this rapid move to digital communications system, there have been significant advances in digital recording devices. Digital versatile disk (DVD) recorders, digital VHS video cassette recorders (D-VHS VCR), CD-ROM recorders (e.g., CD-R and CD-RW), MP3 recording devices, and hard disk-based recording units are but merely representative of the digital recording devices that are capable of

producing high quality recordings and copies thereof, without the generational degradation (i.e., increased degradation between successive copies) known in the analog counterparts. The combination of movement towards digital communication systems and digital recording devices poses a concern to content providers such as the motion picture and music industries, who desire to prevent the unauthorized and uncontrolled copying of copyrighted, or otherwise protected, material.

In response, there is a movement to require service providers, such as terrestrial broadcast, cable and direct broadcast satellite (DBS) companies, and companies having Internet sites which provide downloadable content, to introduce protection schemes. Two such copy protection systems have been proposed by the 5C group of the Data Hiding Sub Group (DHSG) (5C comprising representatives of Sony, Hitachi, Toshiba, Matsushita, and Intel) and the Data Transmission Discussion Group (DTDG), which are industry committee sub-groups of the Copy Protection Technical Working Group (CPTWG). The CPTWG represents the content providers, computer and consumer electronic product manufacturers.

The DTDG Digital Transmission Copy Protection (DTCP) proposal is targeted for protecting copy-protected digital content, which is transferred between digital devices connected via a digital transmission medium such as an IEEE 1394 serial bus. Device-based, the proposal uses symmetric key cryptographic techniques to encode components of a compliant device. This allows for the authentication of any digital device prior to the

0605045 - 080398.P253

transmission of the digital content in order to determine whether the device is compliant. The digital content is itself encoded prior to transmission so that unauthorized copying of the content will result in copy having an unintelligible format.

Thus, even today, the functionality of digital devices such as set-top boxes, digital televisions, digital audio players, and similar such digital devices extends beyond their historical role of conditional access (CA), i.e., merely descrambling content to a CA-clear format for real-time viewing and/or listening, and now include constraints and conditions on the recording and playback of such digital content. For example, currently, copying of scrambled content for subsequent descrambling and viewing or listening may be permitted with the appropriate service/content provider authorization or key provided to the digital device.

0550450 - 0254500

SUMMARY OF THE INVENTION

A method of revoking a descrambling privilege for copy controlled content to a host device is provided. The method includes receiving copy controlled content at a conditional access module. A revocation list is also received at the module. The method includes determining whether the host device associated with the module is on the list. If so, the conditional access module will not descramble the content.

050568.0250

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not by way of limitation in the figures of the accompanying drawings, in which like references indicate similar elements and in which:

Figure 1 is a block diagram of an exemplary entertainment system including one embodiment of a digital device;

Figure 2 is a block diagram of one embodiment of a digital receiver of the digital device;

Figure 3 shows an embodiment of an ECM that includes a CRL version number; and

Figure 4 shows an embodiment of a method of revoking.

09504968 .021500

DETAILED DESCRIPTION

Figure 1 is a block diagram of an entertainment system 100 including one embodiment of the copy management system of the present invention. The entertainment system 100 includes a digital device 110 for receiving a digital bitstream including program data from one or more service providers. Such service or content providers can include terrestrial broadcasters, cable operators, direct broadcast satellite (DBS) companies, companies providing content for download via the Internet, or any similar such content and/or service provider. The program data may include system information, entitlement control messages, entitlement management messages, content, and other data, each of which will be described briefly. System information may include information on program names, time of broadcast, source, and a method of retrieval and decoding, and well as copy management commands that provide digital receivers and other devices with information that will control how and when program data may be replayed, retransmitted and/or recorded. These copy management commands may also be transmitted along with entitlement control messages (ECM), which are generally used by the conditional access unit to regulate access to a particular channel or service. Entitlement management messages (EMM) may be used to deliver privileges to the digital receiver 111 such as rights, access parameters, and descrambling keys. As known, a decryption key is generally a code that is required to restore scrambled data, and may be a function of the rights granted. Finally, content in the program data stream

080398-0245000

may include audio and video data, which may be in a scrambled or clear format.

The digital device or host may be a device within a group including a set top box, television, video player, video recorder, hand disk player, hard disk recorder, personal computer, memory stick recorder, minidisk player, minidisk recorder, digital video disk (DVD) player, DVD recorder, compact disk (CD) player, and CD recorder.

The digital device or host 110 includes a digital receiver 111, which processes the incoming bitstream, extracts the program data therefrom, and provides the program data in a viewable format. The thus extracted program data is then provided to a decoding unit 112 for further processing, including separation of the system information from the content, as well as decoding, or decompressing, of the content to its original form. The digital receiver 111 also regulates access to the program data by other components on the entertainment system 100, and according to one embodiment of the present invention, supports the simultaneous transmission of program data having content in a descrambled format (hereinafter referred to as "descrambled content") and program data having content in a scrambled format (hereinafter referred to as "scrambled content").

According to one embodiment of the present invention, the digital device 110 is a digital television set where the digital receiver 111 is a set-top box integrated therein, and the decoding unit 112 is an MPEG (Motion Picture Experts Group) decoder. The digital television set's display (not

080398.P253

shown) is, according to this embodiment, integrated within the digital device 110. Alternatively, it will be appreciated that the digital device 110 may include only the digital receiver 111 and/or the decoder unit 112, with a display being external to the decoding device 110. An example of this embodiment would be an integrated receiver/decoder (IRD) such as a stand-alone set-top box which outputs NTSC, PAL or Y_pB_pR signals. All such embodiments are included within the scope of the present invention.

Digital device 110 may be coupled to other components in the entertainment system 100 via a transmission medium 120. The transmission medium 120 operates to transmit control information and data including program data between the digital device 110 and other components in the entertainment system 100. It will be appreciated that the entertainment system 100 of Figure 1 is merely an exemplary embodiment, and that other analog and/or digital components may be added or substituted for the components briefly described hereinafter.

Referring to Figure 1, the entertainment system 100 may include an audio system 130 coupled to the transmission medium 120. The audio system 130 may include speakers and an audio player/recorder such as a compact disc player, a Sony MiniDisc® player, or other magneto-optical disc that may be used to play and/or record audio data. A digital VCR 140, such as a D-VHS VCR, may also be coupled to the digital device 110 and other components of the entertainment system 100 through the transmission medium 120. As known, the digital VCR 140 may be used to record analog or digital audio, video, and other data transmissions, and according to an

080398.P253

embodiment of the present invention, may be used to record program data received by the digital device 110 and transmitted to the digital VCR over transmission medium 120.

A hard disk recording unit 150 may also be coupled to digital device 110 and other components via transmission medium 120. The hard disk recording unit 150 may be a personal computer system, a stand-alone hard disk recording unit, or other hard disk recording device capable of recording analog or digital audio, video and data transmissions. As with digital VCR 140, according to one embodiment of the present invention, the hard disk recording unit 150, may be used to record program data received by the digital device 110 and transmitted to the hard disk recording unit 150 over transmission medium 120.

Display 160 may include a high definition television display, a monitor or other device capable of processing digital video signals. In an embodiment where the digital device 110 is a stand-alone set-top box, display 160 may be a digital television set.

Finally, a control unit 170 may be coupled to the transmission medium 120. The control unit 170 may be used to coordinate and control the operation of some or each of the components on the entertainment system 100, as well and other electronic devices remotely coupled thereto.

Figure 2 is a block diagram of one embodiment of the digital receiver 111 including the copy management system according to the present invention. The digital receiver 111 includes a central processing unit (CPU) 210, which controls the overall operation of the digital receiver 111, and

080398.P253

determines the frequency in which a selected channel is broadcast or otherwise transmitted. This information is then transmitted to a tuner 220, which then selects the appropriate frequency of the terrestrial, cable, satellite, or Internet transmission in which to receive the incoming digital bitstream, including program data. The CPU 210 may also support a graphical user interface (GUI), such as an electronic programming guide (EPG), the latter allowing a user to navigate through various channels and program options to select a desired channel or program for viewing, listening, recording and the like. The GUI may be displayed on either a display (not shown) of digital device 110 (e.g., where digital device 110 is a digital television set), or on display 160 (e.g., where digital device 110 is a stand-alone set-top box).

Once the tuner 220 has selected the appropriate frequency, it amplifies the incoming digital bitstream, and provides the output bitstream to a demodulator unit 230. The demodulator unit 230 receives the bitstream from the tuner 220 and demodulates the bitstream to provide program data as originally transmitted. The type of demodulation effected by the demodulator unit 230 will of course depend on the type of transmission as well as the modulation process used in the transmission process. For example, in the case of cable transmissions and Internet transmissions received over cable modems, the demodulator unit 230 may perform quadrature amplitude demodulation (QAD), while for satellite broadcasts, quadrature phase shift key (QPSK) demodulation will likely be required. Terrestrial broadcasts, will likely require vestigial side band (VSB)

080398.P253

demodulation. The present invention is not limited to any one type of transmission and modulation/demodulation scheme, and other schemes are within the scope and spirit of the present invention. In addition to effecting the demodulation process, demodulator unit 230 may also perform error correction on the received bitstream.

The thus demodulated bitstream is now preferably provided to a conditional access unit 240. (That portion of the demodulated bitstream that is not encrypted may bypass the conditional access unit 240 and be provided directly to the demultiplexer 250 as shown by the dashed lines in Figure 2. This might also be the case where none of the bitstream needs decrypting, and/or where there is no conditional access module). The conditional access unit 240 generally performs key management and decryption, as well as descrambling functions as follows.

Typically, if the CPU 210 determines that the program data in the digital bitstream includes scrambled content, that program data is provided to a conditional access unit 240. At this point the CPU 210 may transmit packet identifier (PID) information to the conditional access unit 240, such PID information informing the conditional access unit 240 where in the program data the ECM may be found. The CPU 210 may instead receive the ECM and deliver it to the conditional access unit 240. Alternatively, the conditional access unit 240 may have demultiplexing capabilities allowing it to directly obtain the location of the ECM from the bitstream itself. As discussed previously, the ECMs regulate a user's access to a particular channel or service, and determines the access rights that are needed to be

held by a receiver 111 in order to grant access. The ECMs may also be used to deliver a decrypting or descrambling key or to deliver information (e.g., an algorithm) as to how to derive a key that may be used to descramble scrambled content. Using such key or information regarding derivation of such key, the conditional access unit 240 may descramble the content contained in the program data. Alternatively, the conditional access unit may provide the key to the demultiplexer 250 which will perform the descrambling.

Importantly, although the conditional access unit 240 is shown as an integral, or embedded, in that both the descrambling and decrypting functions are effected internally in receiver 111, the conditional access unit may also split or external. An external conditional access unit descrambles the program data content and decrypts the keys externally; e.g., as is the case with the National Renewable Security System (NRSS) conditional access modules. In a split conditional access unit, the program data content is descrambled within the digital receiver 111, while the key decryption is completed externally, e.g., via a "smart card." All of these systems are intended to be within the spirit and scope of the present invention.

Once the conditional access unit 240 descrambles the program data content, the program data is input to demultiplexer unit 250, which separates the system information from the content in the program data. According to an embodiment of the demultiplexer unit 250, the demultiplexer unit 250 parses the program data for PIDs that are associated with system information, audio information, and video information, and then transmits the

080398.P253

system information to the CPU 210 and the audio and video information to the decoder unit 112. In accordance with one embodiment of the present invention, a digital interface unit 260 is coupled to the conditional access unit 240. Operation of this unit, which allows the receiver 111 to communicate with other digital components in the entertainment system 100, will be discussed at a later point.

The CPU 210, tuner 220, demodulator unit 230, conditional access unit 240, demultiplexer unit 250, and digital interface unit 260 may be implemented using any known technique or circuitry. In one embodiment of the present invention, the CPU 210, tuner 220, demodulator unit 230, demultiplexer unit 250, and digital interface unit 260 all reside in a single housing, while the conditional access unit 240 may reside in an external NRSS-A or NRSS-B conditional access module (as discussed above). Alternatively, the conditional access unit can take the form factor of a Personal Computer Memory Card International Association (PCMCIA) Type II card or a smart card or the like. For example, the conditional access unit may take the form of a Point of Deployment (POD) module or an ISO 7816 smart card.

The content of a digital program may be transmitted in scrambled form. In order for a conditional access unit to recover the scrambled content and permit a person to view the content in clear form, the unit must have the necessary access requirements associated with the scrambled content. An access requirement includes a message that describes the features that the conditional access unit must have in order to decode the scrambled content.

The scrambled content may be referred to as "copy controlled content." For example, a certain key may be needed to view the content. Alternatively, a service tag associated with a given content provider may be required. Technical requirements such as a particular descrambling method may also be required and included as a part of the access requirements. The access requirements associated with a particular program may be transmitted to a conditional access unit along with the program.

Thus, after the host 110 has the access requirements necessary to view a given program content, the host 110 has access to display the content in the clear on display 160 unless that host's access has been revoked. When the host's access has been revoked, the revocation information is sent to a conditional access (CA) unit 240 associated with the host. The revocation information is sent to the CA unit 240 in a certified revocation list (CRL), which may be trickled out over a network. The network may be a home network using a Universal Serial Bus, Blue Tooth, and Panel Link communication mediums. The revocation information includes a list of hosts whose access has been revoked. In one embodiment, the revocation is for the entire service. Alternatively, the revocation may be limited to a specific content provider, such as HBO for example, thus allowing the host to display the content of other channels that have not been revoked.

The revocation list is sent to the CA unit 240 on a well known packet identifier (PID). In a cable network system, the certificate revocation lists may be sent in-band, along with the program content, which allows for

easier time shifting by bitstream recorders. Alternatively, the CRL may be sent to the CA unit in an out of band (OOB) channel, by telephone wires, or by a modem if sent OOB, then it can be delivered to multicast IP addresses. The revocation list can be received and read in real time. Thus, the CRL does not need to be stored, which reduces the overall system memory requirements.

The revocation lists can be divided into lists for different groups of hosts. Multiple lists, where each list corresponds to a different group of hosts, can be sent to the CA units. The CA unit only has to read the list for the corresponding host's group. For example, if the host identifier (ID) is a numeric value, then the range of the host IDs in a given list can be used by the CA unit to quickly determine whether the given list may contain revocation information for the corresponding host. Thus, the CA module can ignore CRLs that have host ID ranges greater than or less than the ID value for the corresponding host of the CA unit.

If the CRL has a range of values that bound the corresponding host's numerical ID value, the CA unit may check the CRL. In one embodiment, the CRL is checked when the CA unit is initially associated with the corresponding host. In another embodiment, the CRL may be checked when a new version of the CRL is sent to the CA unit. The CA module can compare the version number of the received CRL with the version number of the last checked CRL stored in the CA unit's memory. If the received version number is greater than the stored version number, the newly received CRL is read to determine whether the host is on the list.

Doc#: 080398.P253

An embodiment of an ECM that includes the CRL version number is shown in Figure 3. The CRL version information includes the CRL version number and reception time, 310. The ECM may further include the encrypted key 320 for descrambling content, access requirements 330, and an optional signature 340. This ECM allows the CA module to know which CRL version number is the current version number. The CRL itself may be formatted as a data structure. In one embodiment, the CRL is formatted as a private syntax information (PSI) data structure, which is well known in the art. The PSI data structure may also be a MPEG PSI data structure.

The information in the CRL may be filtered and read by either the host or the CA unit. The CA module determines whether the host device appears on the list. Also, if the host device has a 1394 digital interface, the host device can use the CRL information to determine whether other devices in the 1394 home network appear on the list. In one embodiment, there may be two lists, where one list is for the CA hosts and 1394 devices, and the other list is for the other devices. The size of the second list would be substantially smaller than the first list, so that it could be stored in the memory of the host and other devices.

If the host for the CA unit is identified in the revocation list, then the CA unit will not decode the scrambled program content for the corresponding host. Whenever a CA unit identities a host in the CRL, the host is marked as revoked in the internal memory of the CA module. The host may be un-revoked if the host does not appear in a subsequent CRL.

The CA unit includes a memory that stores the revocation status for a plurality of hosts that the CA unit has been connected to. Also, the CA unit can determine the revocation status of program content that has been stored in scrambled form in a digital memory, such as tape for example. If the version number of the CRL stored on the tape is smaller than the version number in the CA unit's memory, then the CA unit will ignore the revocation information stored on the tape.

Alternatively, the CA unit can speculatively and tentatively descramble the program content for a given period of time before the CA unit receives the revocation list. For example, if the CA unit has not received a CRL for the host, the CA unit can descramble the scrambled content for a given period of time, called a timeout period. The timeout period can be determined at the headend or broadcast station, and sent to the CA unit in an ECM. The timeout period may be long enough for the CA unit to receive the CRL multiple times before the timeout period ends, but short enough so that a pirate may not receive significant portions of the content before the timeout period ends.

The timeout counter, once started, will continue to count down to the end of the timeout period, even if a user changes the content that is descrambled, for example, by changing the channel of the tuner. If the CA unit checks the CRL list for the host during the timeout period and the host is not on the list, then the CA unit may continue to descramble the program content. If the host is on the list, then the CA unit ceases to descramble.

Also, if the timeout period ends before the CA unit checks the CRL, the CA unit stops descrambling the program content.

Figure 4 shows an embodiment of a method of revoking. Scrambled copy controlled content is received at a conditional access module, 410, a revocation list is received at the module, 420. The method includes determining whether the host device is associated with the module is on the list, 430. If so, the method causes the conditional access module to deny the content controlled to the host device, 440. The conditional access module may also not descramble the copy controlled content.

While the invention is described in terms of embodiments in a specific system environment, those of ordinary skill in the art will recognize that the invention can be practiced, with modification, in other and different hardware and software environments within the spirit and scope of the appended claims.